e-Safety in Education: A discussion document on Standards, Liability and the Implications of Local Control

Introduction

It is widely recognised in the education community that there is a requirement to explain the complex legal environment with regards to e-safety in education - specifically as it relates to the technology and processes that can be used to control, interdict and protect pupils and staff.

The closure of Becta (the education technology body) and the movement of its e-safety brief to the Department of Education has created an opportunity to begin to clarify and explain this situation.

This discussion document specifically relates to web content filtering technology and is a pre-cursor to a series of white papers researched and produced by Dr. Brian Bandey, the eminent and internationally recognised expert in e-Safety law. It presents two central questions:

- What level of performance is required in web filtering solutions to meet/exceed the legal threshold for delivering suitable protection?

- Where are the boundaries of liability for local authorities, school/academy governors, head teachers and network managers when delivering web access to pupils and staff?

1. e-Safety and web filtering standards for education

It can be argued that the web filtering standard set by Becta (see Addendum 1) should be considered as the technical minimum threshold for safe internet access for children and staff in education as no other implementable standard currently exists.

The Becta accreditation standard for web content filtering products or services is based upon consistently achieving set of challenging criteria. The product or service must block 100% of illegal material identified by the Internet Watch Foundation (CAIC) List. And, it must be capable of blocking at least 90% of inappropriate internet content in each the following categories:

- Adult: content containing sexually explicit images, video or text, the depiction of actual or realistic sexual activity
- Violence: content containing graphically violent images, video or text
- Race hate material: content which promotes violence or attack on individuals or institutions on the basis of religious, racial or gender grounds
- Illegal drug taking and the promotion of illegal drug use: content relating to the use or promotion of illegal drugs or misuse of prescription drugs
- Criminal skill/activity: content relating to the promotion of criminal and other activities
- Gambling: content relating to the use of online gambling websites or information relating to the promotion of gambling and gambling advice

The process used to test filtering threshold compliance is based upon the testing body submitting a number of known URLs (covering the above subjects) designed to deliver both positive and false-positive outcomes.

In addition, the solution is required to be constantly updated (with blocklists) and provide adequate protection against; external malicious attacks, viruses, malware, email borne threats and denial of service attacks. This specification is coupled with a rigorous technical analysis of the product/service and an assessment of the supplier's ability to execute and support their offering effectively.

Independently Certified e-Safety Products and Services

In the majority of cases the actual filtering capability of a product or service cannot be determined by the IT professional that integrates it into a network (or in many cases the software vendor who develops it) without deferring to independent certification or evaluation. The testing process requires high levels of expertise in filtering technology, a replicable and auditable process and access to a wide variety of pre-tested benchmark URLs which point to 'typical' content. On this basis, the selection of an e-safety solution that at the outset seems more attractive on price, performance, features or functionality may not (when examined against the legal obligations of the School) meet the threshold required to protect the pupil and the individuals/organisation that has the duty to care for them.

If 'self-testing' approach is undertaken when selecting an e-Safety and filtering solution, it is recommended that the specifier should consider and weigh all of the elements, vectors and situations that could cause harm in the internet environment that the pupils and staff will have access to (a significant task). They should then produce a comprehensive e-Safety Risk Assessment as is required by Health & Safety Law.

It is worth emphasising at this point that the Law of Negligence currently sets thresholds of legal liability using well-understood and clear criteria. Additionally, Health & Safety Law places obligations on Schools to make regular e-risk assessments and to reduce the e-safety risk as low as reasonably possible (ALARP) – on this basis there is little ambiguity in the Law with regards to providing adequate e-safety for pupils.

In summary, it appears that considering a filtering solution to be 'good enough', assuming its capability or deferring to a suppliers own stated capability may not be an adequate strategy when dealing with the complex intersection of e-safety technology and the legal liabilities created by Child Protection, Health & Safety, Negligence and Criminal Law.

2. Liability for breaches of e-safety Law in schools

The changes in school organisations (such as the development of new Academies) and the increasingly localised specification and provision of services has created groups of individuals that are becoming directly responsible and personally liable under existing legislation for e-safety within their organisations. Existing organisations already have individuals that carry this clearly defined responsibility possibly without their knowledge or full understanding of its implications.

The requirement for providing suitable protection and fulfilling the matrix of legal obligations within the e-safety environment is necessarily high and far reaching. The penalties for failing to meet the standards prescribed by e-Safety Law fall within, for example, Health and Safety Law, the Law of Negligence and the Criminal Law system. These penalties can directly impact both the organisation itself and certain individuals within organisations such as policy makers, boards of governors, head teachers and other decision-makers within local education organisations.

A chain of trust

In this complex environment, it is important to emphasise that education professionals are professionals in educating children - not IT systems or the Law. As a function of their role they choose to expose the children under their charge to the risks associated with internet access - the Law therefore looks to them to manage the risk to which they are exposing the children. In managing this risk they rely extensively on technical solutions supplied by their supporting IT professionals (to create a safe on-line environment). In turn, the IT professionals rely upon supplier statements of effectiveness, forms of external verification (such as Becta accreditation) and a measure of internal 'testing' of filtering and other capabilities. The supplier (software/system vendor in this case) does not bear legal health & safety responsibility for damage caused to an individual or group of individuals from the quality (or lack of it) of their solution – ultimate responsibility and liability remains with the organisation (and individuals) that implement and operate their system. This extended chain of trust is likely to be thoroughly tested (in a legal and technical sense) in the aftermath of any serious e-safety incident.

Providing adequate protection for all

Short of locking down access to the internet (a contravention of Ofsted's guidance to 'encourage and support schools to move from locked down to managed [e-safety] systems') the most practical solution to providing effective e-safety for pupils/staff and providing effective protection for organisations and their staff is to implement a solution that can be shown to meet or exceed a high and recognised standard of web filtering.

3. Local responsibility for local e-safety solutions

Organisations considering moving from local authority / centrally provided e-safety solutions need to provide both a safe environment and tangible benefits of operating independently of the LA technical and legal framework.

Currently web filtering and e-safety software is often delivered as a bundled component of connectivity and other centrally delivered services (such as email, telephony, anti-virus/anti-malware). It is often 'forced' upon the recipient organisation and the proffered solution often does not meet either the filtering capability threshold or the functionality/feature requirements required.

In this situation effective replacement systems, software and IT infrastructure requirements can be specified and implemented with confidence by experienced local network managers. And, the benefits calculation (to leave centrally provided services) can be relatively simple to perform and the outcome both financially and in a productivity sense can be made clear to governing bodies and other stakeholders.

However, the choice of e-safety software requires careful consideration as it has direct legal implications to the organisation and its staff and serious safety implications to its pupils. As discussed previously, selecting a solution based on any other criteria (ease of use, management, flexibility, price etc) than its proven effectiveness at providing a safe environment may create unintended and significant liabilities in the unfortunate event of a serious e-safety incident.

Notes on Becta Accredited Web Filtering Solutions

About Becta

Becta provided the leadership which enabled effective use of technology across the education system in the most coherent, cost-effective way – the e-Safety brief has now been passed to the Department of Education. They ensured the market developed products and services met the needs of the education and skills sector and provided value for money.

Their rigorous research and evaluation enabled organisations to evaluate the impact of technology on the education and skills system; And, provided expert, independent advice helping the front line helping make informed choices about technology and plan, buy and use it effectively. Their expertise enabled learners and their families access technology, get involved in learning and stay safe on-line. They also provided practical tools that saved time and money, improved teaching and learning and helped to share best practice.

Becta Accreditation

The Becta Accreditation of Internet Services and Products enabled schools and other establishments to make an informed choice of a managed internet service provider or web content filtering solutions. Becta accredited products and services must meet and maintain specific standards in web content filtering and service performance.

The standards of assessment have been developed in consultation with partners in education and industry to ensure the provision of reliable and relevant information. The scope of the accreditation has been extended to include a wider range of standalone products designed to protect internet users not just in the school environment, but which can also be employed in other environments where children and young people have access to the internet.

A managed internet service provider is a provider to education that can supply a range of internet safety services. An individual web content filtering product or service supplies specific solutions to internet services providers.

About the Becta Web Filtering Accreditation Standards:

Accreditation is awarded to either managed internet services or internet products. Accredited suppliers are either: accredited managed internet services: these offer internet access and a range of internet safety services. Managed internet services are those provided by commercial ISPs, local authorities and regional broadband consortia. accredited web content filtering products or services: these supply specific solutions to ISPs and may be provided as a managed service to its customer.

Many of the internet services are jointly provided by commercial and public-sector organisations. For example, the telecommunication and internet access aspect may be supplied by a commercial entity, but the filtering of unsuitable internet content may be provided by a local authority. Becta web content filtering products and services requirements.

A web content filtering product or service must meet or exceed the following requirements as a minimum under the Becta Accreditation of Internet Services. Internet Watch Foundation Child Sexual Abuse Images and Content (CAIC) list.

It is a requirement of this accreditation that the Internet Watch Foundation CAIC list is implemented in all accredited products and services.

Illegal content blocked

The product or service must block 100% of illegal material identified by the Internet Watch Foundation.

Inappropriate content blocked

The product or service must be capable of blocking at least 90% of inappropriate internet content in each the following categories:

- Adult: content containing sexually explicit images, video or text, the depiction of actual or realistic sexual activity
- Violence: content containing graphically violent images, video or text
- Race hate material: content which promotes violence or attack on individuals or institutions on the basis of religious, racial or gender grounds
- Illegal drug taking and the promotion of illegal drug use: content relating to the use or promotion of illegal drugs or misuse of prescription drugs
- Criminal skill/activity: content relating to the promotion of criminal and other activities
- Gambling: content relating to the use of online gambling websites or information relating to the promotion of gambling and gambling advice.

Changes requests to the filtered content

- The must be a mechanism for an authorised member of a customer organisation to request amendments to the web content filtering service
- The appropriate procedures must be in place to authenticate personnel that request changes to any part of the service.

Security and virus protection

The service or product should include adequate protection against the following:

- External malicious attacks
- Viruses and trojans
- Denial of service attacks
- Email bombs and spam

Support requirements

- Support must be available through two channels: telephone and e-support (e-support includes email and or web based contact methods)
- All support requests must be acknowledged within two working hours and assigned a unique reference number
- A first attempt to resolve the support request takes place within the first four hours

Other areas that require compliance include system availability and capacity, service continuity, service management, customer service and requirements for Becta to have the appropriate access to any given service or product to enable monitoring evaluations to take place at any time during the accreditation period.

About Dr. Brian Bandey

As an internationally recognised expert in e-Safety law Dr. Brian Bandey has partnered with Smoothwall to advance his technical legal research into the Legal Exposure that arises for Educational Establishments and their Staff through Pupil misuse of School information and communication technology. This complex and enveloping "Threat Landscape" is not well understood – it consists of the intersection of established areas of law which include; the Law of Negligence, Heath & Safety Law and Criminal Law (amongst others).

Dr. Bandey's current research is mapping the Threat Landscape and revealing what the imminent exposure of employees and organisations is, together with giving 'real-life' answers to the issues raised.

In addition, Dr. Bandey is one of the United Kingdom's leading experts on Computer and Internet Law and the international application of the Law of Copyright to Computer and Internet Programming Technologies. His work is published throughout the world, he is a scholar at the University of Oxford, England and a Research Contributor to the Oxford Intellectual Property Research Centre.

About Smoothwall

Smoothwall is an established web security technology company – its primary focus is providing web filtering and security systems for the education, government and enterprise market spaces.

More Information

For more information on this subject please visit: www.smoothwall.net & www.drbandey.com